



Department of Homeland Security Daily Open Source Infrastructure Report for 16 February 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The Charlotte Observer reports thieves have stolen more than 3,500 pounds of copper — worth about \$7,500 — from seven electric substations in four North Carolina counties: Burke, Catawba, Cleveland, and Lincoln. (See item [1](#))
- The Associated Press reports the federal government has announced a crackdown on people who shine laser beams at planes landing at Detroit Metropolitan Airport after receiving reports of 16 pilots complaining of such beams on Monday evening, February 13. (See item [11](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) — <http://www.esisac.com>]

1. *February 15, Charlotte Observer (NC)* — **Thieves stealing electric company's equipment.** Thieves have stolen more than 3,500 pounds of copper — worth about \$7,500 — from seven electric substations in four North Carolina counties, a rural electric cooperative manager said Tuesday, February 14. Between 500 and 600 pounds were taken from each substation in the last four months, said Colon Saunders, manager of operations for the Rutherford Electric Membership Corp. The cooperative has about 64,000 customers in parts of 10 counties. The substations are in Burke, Catawba, Cleveland, and Lincoln counties and serve about 8,000 people in areas along NC 18, NC 27, and NC 10. Copper protects equipment from power surges

from lightning strikes. The thefts haven't led to any equipment damage or service interruptions, Saunders said. Thieves crawled under or cut through fences, he said, then used bolt cutters or socket wrenches to remove strips as long as 15 and 20 feet from the unmanned substations. The thieves likely are selling the metal to dealers, he said, with copper now worth about \$2.10 a pound. "That's about as high as it's ever been," Saunders said. The company has increased inspections at the substations and is working on better motion sensors to alert people monitoring the sites at company headquarters.

Source: <http://www.charlotte.com/mld/observer/news/local/13874923.htm>

2. *February 15, Charlotte Observer (NC)* — **Duke Power Company defends ice storm response.** Duke Power Company officials say their crews reacted promptly and appropriately following a December 15 ice storm that knocked out power to 900,000 customers in the Carolinas. Charlotte-based Duke Power made the comments in a 96-page report to a South Carolina state agency that represents the public in utility cases. The agency, the Office of Regulatory Staff, had asked for a response following numerous complaints by the public in the days following the ice storm. Dukes Scott, executive director of the agency, said his group will look at Duke Power's response and "determine where there is room for improvement in Duke Power's infrastructure, operations and response." Some customers lost power for up to a week. Officials said two issues contributed to telephone problems and busy signals for customers reporting outages. They said BellSouth experienced "extremely high" call volumes during the storm's first day and took steps to limit calls, to protect its equipment from overload and failure. Also, an error with Duke's toll-free service provider resulted in unnecessary busy signals. Duke Power said it restored power to 98 percent of affected customers by December 20 and all power by December 22, a week after the storm.

Source: <http://www.charlotte.com/mld/charlotte/13877670.htm>

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

3. *February 15, York Weekly (ME)* — **Utility truck accident prompts roadway closure.** On Saturday, February 11, at 7:01 a.m. EST, the York Police and York Beach Fire Departments responded to a motor vehicle accident on Route 1 near the Ogunquit, ME, town line. Units arriving on scene were confronted with a utility truck that had flipped on its side. Inside the vehicle were three chemicals: freon, nitrogen and acetylene. Suspicion of a leak prompted fire officials to call in the York County Hazmat Team to help open the vehicle and remove the chemicals. Also responding to the scene was the Ogunquit Rescue and Decontamination Unit as well as the Hazmat team from the Portsmouth Naval Shipyard (PNS). The PNS team tested for chemical leaks and when none was detected, the roof of the utility truck and the chemicals were removed. Route 1 was closed from 7:45 to 9:40 a.m. EST that day.

Source: <http://www.seacoastonline.com/news/yorkweekly/02152006/news/88006.htm>

4. *February 09, Daily News Transcript (MA)* — **Break in gas line forces mall evacuation.** A construction crew at Natick Mall in Natick, MA, hit a two-inch gas line with an excavating machine Wednesday morning, February 8, forcing the evacuation of all mall employees before doors were opened to the public. After the pipe broke, the heat and air conditioning system at the mall's Flutie Pass entrance sucked gas into the building, said Deputy Fire Chief Richard

White. The problem, however, was resolved quickly and no one was injured, he said. The accident happened around 8:45 a.m. EST, when construction workers were digging an area of the mall's expansion site and hit a gas pipe they thought ran straight but, in fact, made a curve, said White.

Source: <http://www3.dailynewstranscript.com/localRegional/view.bg?articleid=71814>

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report.

[\[Return to top\]](#)

Banking and Finance Sector

5. *February 15, Associated Press* — **Brazilian police identify hacker gang.** Brazilian police arrested 41 hackers Wednesday, February 15, accused of using the Internet to divert millions of dollars out of other people's bank accounts. Some 200 federal police were deployed to serve 65 arrest warrants against a gang of hackers mostly operating in Campina Grande. Arrests also were made in six other states. Police said over the past three months the gang invaded approximately 200 accounts in six banks, stealing millions of dollars using a Trojan horse virus sent via e-mail. The program entered computers and, working in the background, copied account numbers and passwords without the users' knowledge. Police said the leader of the gang was a 19-year-old and five of those arrested so far were minors. Police were still looking for 24 other alleged gang members.

Source: <http://www.theage.com.au/news/breaking/brazilian-police-bust-hacker-gang/2006/02/15/1139890794432.html>

6. *February 14, InformationWeek* — **Crimeware nearly doubles in December.** A recently revealed image-rendering vulnerability related to Windows Meta Files made it easier for phishers to spread software designed for a criminal enterprise, such as identity theft. The number of sites distributing "crimeware" — or software engineered for criminal activity like identity theft or information fraud — nearly doubled in December, rising from 4,630 in November to 7,197 the following month, according to a report issued Tuesday, February 14 by the Anti-Phishing Working Group (APWG). APWG Chairperson David Jevans said, "The speed, precision and massive scale by which the phishers were able to identify and exploit this vulnerability for criminal enterprise highlights the fact that the e-Crime industry has reached a level of efficiency that has the potential to threaten the larger online economy." Crimeware exploitation can be thought of as an automated form of phishing. According to the APWG, a recently revealed image-rendering vulnerability related to Windows Meta Files made it easier for phishers to spread crimeware. During the month of December, more brand-spoofing subterfuges were recorded than any other month on record. The vast majority of those attacks — 89.3 percent — targeted the financial industry, most of which involved seven major brands.

Source: <http://www.informationweek.com/story/showArticle.jhtml?articleID=180201747>

7.

February 14, The Guardian (UK) — **Nigerian scammer jailed.** A Nigerian 419er was jailed Friday, February 10, for 376 years by a Lagos court for "stealing, forgery, impersonation and conspiracy to obtain money by false pretences" contrary to the Advance Fee Fraud Act. Harrison Odiawa, 38, also known as Abu Belgori, managed to extract \$1,939,710 from U.S. national George Robert Blake on the promise of a percentage of a bogus \$20.45 million Ministry of Health contract. The classic advance fee scam (also known as the "419" or Nigerian scam) saw a duped Blake transfer the "advance payments" after seeing forged documents — including a certificate of registration with the Corporate Affairs Ministry and the aforementioned forged Ministry contract — which convinced him he was indeed about to get rich. Blake raised the cash from his company, Quest Exploration and Development, and his own personal assets. Odiawa was eventually tracked and arrested in Lagos by Economic and Financial Crime Commission (EFCC) operatives. The 419er was convicted on 48 of the 58 counts on which he was charged, and was also ordered to pay back \$1.6 million to his victim. Blake has already served a 30-month jail sentence in the U.S. for money laundering and bank wire offenses.

Source: http://www.theregister.co.uk/2006/02/14/419er_jailed/

8. *February 13, Washington Post* — **The new face of phishing.** A new type of phishing attack targeting the tiny Mountain America credit union in Salt Lake City, UT, has been spreading. The scam arrives in an HTML-based e-mail telling recipients that their Mountain America credit union card was automatically enrolled in the Verified by Visa program, a legitimate security program offered by Visa that is supposed to provide "reassurance that only you can use your Visa card online." The e-mail includes the first five digits of the "enrolled card," but those five digits are found on all Mountain America bank cards, so that portion of the scam is likely to be highly convincing for some recipients. The message directs readers to click on a link and activate their new Verified by Visa membership. The phishing site is protected by a Secure Sockets Layer (SSL) encryption certificate issued by the credit reporting bureau Equifax that is now part of Geotrust. All legitimate banking sites use SSLs, but it's rare to see them on fraudulent sites. Geotrust and other SSL issuers do due diligence to ensure that the entity requesting an SSL certificate is indeed authorized. In this case, however, the user can view more information about the site's security and authenticity.

Source: http://blog.washingtonpost.com/securityfix/2006/02/the_new_face_of_phishing_1.html

9. *February 13, WLKY-32 (IN)* — **Police make arrest in \$100,000 counterfeit ring; more people may be involved.** After allegedly writing more than \$100,000 worth of bad checks, an Indiana man is now behind bars. State police arrested Lance Gilner, who, investigators said, was writing hot checks all over southern Indiana for several months. Gilner, 36, was arrested in November, but an ongoing investigation kept detectives from releasing details about the case until Monday, February 13. "You can buy the paper with water marks, and that's what businesses look for," Indiana State Police Sgt. Jerry Goodin said. Although investigators have Gilner behind bars, they're still warning area businesses to be aware because he might be one member of a larger counterfeiting ring in southern Indiana, Cornell reported.

Source: http://www.wlky.com/news/7015754/detail.html?rss=lou&psp=new_s

[[Return to top](#)]

Transportation and Border Security Sector

10. *February 15, Chicago Sun–Times* — FAA giving air traffic controllers cushion of error.

Beginning at the end of the month, planes approaching Chicago–area airports will be allowed to fly closer together as part of a new policy the Federal Aviation Administration (FAA) is testing. Current policy requires that most planes lining up on their final approach to an airport be separated horizontally by three miles. That won't change, but during a 90–day trial set to begin February 27, air traffic controllers at the Terminal Radar Approach Control center in Elgin, IL, won't be charged with operational errors for planes at least 2.7 miles apart. Three or more operational errors can cost a controller his or her job or certification, FAA spokesperson Greg Martin said. The new policy provides a buffer for air traffic controllers without compromising passenger safety, controllers and FAA officials said. Whether because of a shift in the wind or a pilot putting the landing gear down early, a plane may slow down on its approach, temporarily reducing separation between planes through no fault of a controller's. Planes at least 2.5 miles apart fall within the margin of safety, Martin said. Still, the FAA will keep an eye on controllers who consistently run planes below the three–mile standard.

Source: <http://www.suntimes.com/output/news/cst-nws-hare15.html>

11. *February 15, Associated Press* — Feds say will crack down on laser pointers at Detroit airport.

The federal government has announced a crackdown on people who shine laser beams at planes landing at Detroit Metropolitan Airport. The Federal Aviation Administration (FAA) received reports of 16 pilots complaining of such beams on Monday evening, February 13, said spokesperson Elizabeth Isham Cory. This was the second such incident at Detroit Metro reported in the last six months. There also were incidents in several states in late 2004 and early 2005. "We treat it as a very serious matter," FBI Special Agent Dawn Clenney said. "Laser beams can disorient pilots responsible for an airplane full of passengers." Pointing laser beams at airplanes could be considered a terrorist act under the law, Clenney said. Conviction would carry a penalty of up to 20 years in prison.

Source: http://www.usatoday.com/travel/flights/2006-02-15-detroit-airport-lasers_x.htm

12. *February 15, Associated Press* — Hawaiian Airlines sues Mesa. Hawaiian Airlines is seeking a court order to block Mesa Air Group's entry into the island market for two years, alleging that the new airline illegally used confidential business data from Hawaiian's bankruptcy. In a complaint filed in U.S. Bankruptcy Court, Hawaiian said the information was key in Mesa's decision to begin inter–island services in April or May. In September, Mesa announced plans to offer one–way fares as low \$43 to compete directly against Hawaiian and Aloha Airlines by offering flights between islands. The lawsuit filed Monday, February 13, seeks unspecified monetary damages and an injunction that would prevent Mesa from offering Hawaii flights for at least two years. Hawaiian says Mesa was given access to more than 2,000 pages of detailed information about Hawaiian's business strategy, pricing structure, passenger counts and quarterly projections through the end of 2007. Hawaiian, which filed for bankruptcy in 2003, emerged from Chapter 11 reorganization last June under the ownership of Ranch Capital LLC.

Source: http://www.usatoday.com/travel/flights/2006-02-15-hawaiian-sues-mesa_x.htm

13. *February 15, Boston Globe* — FAA cancels runway drills at Boston's Logan. The Federal Aviation Administration (FAA) on Tuesday, February 14, abruptly canceled plans to test and calibrate a new computer upgrade to Logan International Airport's ground radar system. The

upgrade is critical to fixing problems that led to a spate of runway incidents at the airport last year. The tests, which would have involved two propeller aircraft repeatedly taking off and landing on intersecting runways while airlines were also using the airport, had been scheduled to begin next week. But, federal aviation safety officials said they would conduct the tests at another airport, which has not been named. Jim Peters, a spokesperson for the FAA, declined to comment when asked whether officials were concerned about the safety of conducting the tests on Logan's intersecting runways while the airport was operating during a busy school vacation week. Logan was the first airport in the nation to have received the software upgrade, part of an effort by the FAA and the Massachusetts Port Authority, which owns and operates the airport, to prevent runway incidents. Logan led the nation last year in occasions in which a plane or vehicle entered or crossed a runway being used by another aircraft.

Source: http://www.boston.com/news/local/massachusetts/articles/2006/02/15/faa_cancels_runway_drills_at_logan/

14. *February 15, Associated Press* — **Study: San Diego border wait cost U.S. \$3.74 billion last year.** Delays at U.S.–Mexico border crossings in San Diego County cost the U.S. economy an estimated \$3.74 billion in lost sales, jobs and productivity last year, according to a study released Tuesday, February 14, by the San Diego Association of Governments and the California Department of Transportation. The report's authors estimated that shoppers, tourists, and commuters spent an average of 45 minutes waiting to cross from Mexico into San Diego County in 2005, which cost the U.S. economy \$2.48 billion. Delayed freight had a broader impact across the United States because about 30 percent of trucks had a final destination outside San Diego County. The report's authors estimated that keeping cargo trucks waiting at the border for an average of two or more hours cost the U.S. economy \$1.26 billion last year. The delays highlighted the challenge facing U.S. officials as they balance demands from growing international trade with post–September 11 national security requirements. In an effort to ease delays for frequent travelers, the government has introduced programs for prescreened truckers and visitors to cross more quickly.

Source: <http://www.thedesertsun.com/apps/pbcs.dll/article?AID=/20060215/NEWS10/602150336/1024>

[[Return to top](#)]

Postal and Shipping Sector

Nothing to report.

[[Return to top](#)]

Agriculture Sector

15. *February 15, Agricultural Research Service* — **Test for barber pole worm.** A test in the form of a plastic card featuring pictures of the eyes of sheep may help thwart the spread of barber pole worm, *Haemonchus contortus*, a parasite of small ruminants that's becoming increasingly resistant to the chemicals used to control it. The test, called the FAMACHA eye color chart, can help sheep and goat producers save money by allowing them to deworm only the animals that need it, according to Agricultural Research Service (ARS) animal scientist Joan Burke. This

would slow the spread of chemical-resistant parasites through more efficient identification, treatment, and removal of infected animals. Barber pole worms are microscopic, blood-sucking pests that thrive in heat and humidity and induce fatal cases of anemia and “bottle jaw” disease in animals. The worms' increasing resistance to control chemicals — a result of widespread use of treatments — now threatens the entire goat and sheep population of the eastern U.S., according to Burke. The chart shows five high-resolution photographs that focus on shades of redness of the inner eyelids of sheep. Pale inner eyelids can be indicative of the parasite's presence. The test was 92 percent accurate in a study conducted on sheep and goats in Arkansas, Georgia, Louisiana, Florida, and the U.S. Virgin Islands.

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

16. *February 15, News Journal (DE)* — **Virus threatens Delmarva chickens.** Treating a highly contagious poultry virus found recently in Delmarva flocks will be costly for Delaware and Maryland farmers and poultry companies. An upper respiratory disease that can kill chickens has spread to about 20 farms in Delaware and six in Maryland. The virus, known as laryngotracheitis (LT) can be controlled by vaccinating flocks. This situation will hurt Delmarva's \$1.6 billion poultry industry. Delaware produced \$686 million worth of broilers last year. Poultry companies will incur a cost for the vaccine, which causes flu-like symptoms in chickens and decreases appetites. As a result, the companies are forced to wait longer for chickens to reach slaughter weight. It is too early to gauge the financial impact of the disease. Vaccinating the birds also is expected to reduce income for poultry growers. "If they are lighter, I get paid less," said Charlie Postles, whose 120,000 Perdue birds in Milford were vaccinated last week. "If I keep them longer and get the weight, I have used more electricity. Either way you look at it, it is going to cost the grower." LT is an airborne virus that attacks the trachea, or wind pipe, and eyes of birds. About 20 percent to 30 percent of untreated birds die from LT. Source: <http://www.delawareonline.com/apps/pbcs.dll/article?AID=/20060215/BUSINESS/602150359/-1/NEWS01>

17. *February 15, Associated Press* — **Bull bison killed after mingling with cattle; two dozen cattle to be tested.** Cattle just north of Yellowstone National Park will be tested for the disease brucellosis after a bull bison was caught among them, Montana state veterinarian, Tom Linfield, said Tuesday, February 14. Linfield said about two dozen cattle that had been vaccinated against brucellosis will be given a blood test, likely this spring. Linfield said that bison have been out among livestock in the area several times already this winter after leaving the park. Authorities killed the bull bison. Blood was taken from the bison to test for brucellosis, Linfield said. Blood tests are used to indicate whether an animal has been exposed to brucellosis. If an animal tests seropositive, that doesn't necessarily mean it is infectious. A culture test of tissues would be used to determine that, Linfield said. Many Yellowstone bison have brucellosis. The potential for transmission of the disease from bison to cattle is at the center of a state-federal management plan that allows for the hazing or capture of bison that migrate into Montana. Brucellosis can cause cows to abort and, should it turn up in cattle, could cost the state its prized brucellosis-free status. Source: http://www.helenair.com/articles/2006/02/15/montana/a0902150_6_01.txt

[[Return to top](#)]

Food Sector

18. *February 13, Food Safety and Inspection Service* — Public meeting on advances in post-harvest reduction of salmonella in poultry. The U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) Monday, February 13, announced a public meeting February 23 to 24 in Atlanta, GA, to hear and discuss presentations on reducing the presence of Salmonella and other enteric microorganisms in poultry slaughter and processing. Since 2002, FSIS has seen an increase in Salmonella positive samples in broilers. Although the overall percentage of positive samples in verification testing of broilers is still below national baseline prevalence figures, the upward trend in recent years is of concern to the agency. In August, FSIS held a public meeting to hear presentations on advances in pre-harvest reduction of Salmonella in poultry. The upcoming meeting in Atlanta will focus on interventions during broiler slaughter as well as further processing of ground chicken and turkey. FSIS will also announce and seek input on strategy to more effectively control Salmonella in all classes of poultry.

Source: http://www.fsis.usda.gov/News_&_Events/NR_021306_02/index.as.p

[\[Return to top\]](#)

Water Sector

19. *February 15, Nepal News* — Maoists disrupt drinking water supply in Dailekh. A group of armed Maoists have shut down two separate drinking water supply projects in Nepal's Narayan municipality in Dailekh district, completely disrupting the drinking water supply in the region, a report said. This is the sixth time that the Maoists have disrupted drinking water supply in the region, the Rajdhani daily reported. The Maoists exploded bombs in the reservoir tanks of Belaspur Drinking Water Project in Kharigoura VDC-8 and in Dailekh Bazaar Drinking Water Project in Bhavani VDC-9. The Maoists also damaged the water supply pipelines of this project, the paper adds. Likewise, eyewitnesses said the Maoists have disrupted the water supply after releasing a written statement demanding the release of the Maoists who were under detention. These two drinking water projects were supplying drinking water to more than 20,000 people in Dailekh Bazaar, Thalu Danda, Bhawani Tole, Purano Bazaar, Nayabazaar, and other places of Narayan municipality.

Source: <http://www.nepalnews.com/archive/2006/feb/feb15/news12.php>

[\[Return to top\]](#)

Public Health Sector

20. *February 15, World Health Organizations* — Counterfeit medicines. The World Health Organization (WHO) calls for immediate concrete action against the growing epidemic of counterfeit medicines. In a bid to accelerate the war on fake drugs, the agency will push for stronger global cooperation, political commitment and creative solutions at a meeting in Rome from February 16 to 18. WHO aims to create a global task force involving all major interested parties. The task force will focus on legislation and law enforcement, trade, risk communications and innovative technology solutions, including public-private initiatives for applying new technologies to the detection of counterfeits and technology transfer to

developing countries. The counterfeiting of medicines is present in all countries and is thought to represent 10 percent of the global medicines trade. These products mostly have no therapeutic benefit; they can cause drug resistance and death. Trade in counterfeits is extremely lucrative, thus making it more attractive to criminal networks.

Source: <http://www.who.int/mediacentre/news/releases/2006/pr09/en/index.html>

21. *February 15, Agence France–Presse* — **H5N1 outbreak confirmed in southern Russia.** The H5N1 bird flu virus has been found among poultry in the southern Russian province of Dagestan, apparently spread by wild birds. "An infection of the bird flu virus type H5N1 occurred" at a poultry farm in the village of Shamkhal, close to the Caspian Sea coastal city of Makhachkala, said the deputy head of Russia's veterinary surveillance department, Nikolai Vlasov on Wednesday, February 15. The outbreak is the first confirmed case of H5N1 in the impoverished and unstable Russian Caucasus region. The virus had previously appeared in several other Russian provinces last year, notably in Siberia, prompting authorities to slaughter hundreds of thousands of birds in an effort to stem its spread. However in recent days the virus has been detected across the Caucasus mountains in neighboring Azerbaijan, while nearby Turkey has recorded 21 cases of the virus in human beings. Russia's agriculture ministry said that monitoring had been stepped up in the Caucasus and experts were to be sent to Dagestan. Source: http://news.yahoo.com/s/afp/20060215/hl_afp/healthflurussia_060215162126;_ylt=AmlM_71Od61sEG8FLOXGVFqJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--
22. *February 15, Associated Press* — **Iraqi health minister declares bird flu alert in southern province.** Iraqi authorities have declared a bird flu alert in a southern province and called for security forces to prevent people from carrying birds in and out of the area, officials said Wednesday, February 15. Iraq's alert is the latest measure taken by health authorities there to combat bird flu following last month's discovery of the country's only confirmed human case of the disease. Minister Abdel Mutalib Mohammed declared the alert after birds suspected of having the disease were discovered in Maysan province, a major southern trade route in Iraq, said Ibtisam Aziz Ali, spokesperson for a government committee on bird flu. Mohammed said the government has to "totally close" Maysan using Iraqi soldiers and police and carry out culling of poultry. "The disease has apparently spread among local birds, not migratory birds," Mohammed said. "I have seen five centers where infections have been detected by rapid laboratory testing. Now we have declared a state of health alert." Maysan includes some of Iraq's famous marshlands, and U.S. and United Nations officials fear the deadly disease could spread rapidly if it reaches the area rich in bird life. Source: <http://www.signonsandiego.com/news/world/20060215-0402-birdflu.html>
23. *February 15, Reuters* — **New Nigerian bird flu cases, panic selling blamed.** Panic selling of birds infected with bird flu has helped spread the H5N1 virus in Nigeria, but compensation could persuade farmers to abide by quarantine rules, a top veterinary expert said on Wednesday, February 15. The H5N1 strain was confirmed last week in four farms in three northern Nigerian states, but there have been suspected outbreaks in at least five other states in Africa's most populous country. The virus poses a major health risk in Nigeria because chickens run free in millions of backyards and are carried live in public transport. Federal authorities have ordered suspect farms to be quarantined, sick birds to be culled, and transport or sale of birds from affected states to stop, but implementation has been slow in some places

and has not happened at all in others. No human case has been found so far. Detecting such a case will be difficult because mortality rates are high from other diseases and health services are almost non-existent in rural areas, where people are often buried without a medical check.

Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=healthNews&storyID=2006-02-15T143435Z_01_L15677409_RTRIDST_0_HEALT H-BIRDFLU-NIGERIA-DC.XML&archived=False

24. *February 14, Agence France-Presse* — **France warned of high risk of bird flu contamination.** The French food safety agency AFSSA warned of a heightened risk of the H5N1 strain of bird flu. France is Europe's biggest poultry producer, with free-range birds accounting for 17 percent of its production — as well as Western Europe's main crossroads for migratory birds. "We have absolutely no control over the introduction of the virus by migratory birds that are about to start returning from Africa to Siberia, Scandinavia, and Greenland. It is unavoidable," AFSSA expert Jean Hars said. "All migratory species either fly over or stop in France," he added. AFSSA warned that "French birds now face a heightened risk of contamination," following the appearance of the virus in Nigeria, and the discovery of infected swans notably in Greece and Italy. The southwestern and western Atlantic coast were at particular risk, AFSSA said, and poultry farmers in those areas were advised to carry out preventive vaccination for any birds left outdoors. The French agriculture ministry has already ordered free-range birds in more than half of its 96 mainland departments to be kept in shelters to reduce the risk of them catching the H5N1 virus from wild birds. Live birds have also been banned from all markets and trade fairs.

Source: <http://www.breitbart.com/news/2006/02/14/060214190409.og1gfg uc.html>

25. *January 06, Academic Emergency Medicine* — **Concept of operations for triage of mechanical ventilation in an epidemic.** The recent outbreak of severe acute respiratory syndrome (SARS) and the growing potential of an influenza pandemic brings into consideration the fact that despite great advances in critical care medicine, the capacity to provide intensive care to the large number of patients that may be generated in an epidemic or multisite bioterrorism event is lacking. Because many epidemic and bioterrorist agent illnesses involve respiratory failure, mechanical ventilation is a frequently required intervention but one that is in limited supply. In advance of such an event, triage criteria that depend on clinical indicators of survivability and resource utilization to allocate scarce health care resources to those who are most likely to benefit should be developed. These criteria must be tiered, flexible, and implemented regionally, rather than institutionally, with the backing of public health agencies and relief of liability. This report provides a sample concept of operations for triage of mechanical ventilation in epidemic situations and discusses some of the ethical principles and pitfalls of such systems.

Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=healthNews&storyID=2006-02-14T201859Z_01_COL473121_RTRIDST_0_HEALT H-VENTILATOR-TRIAGE-DC.XML&archived=False

[[Return to top](#)]

Government Sector

26.

February 15, U.S. House of Representatives — **A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina.** On September 15, 2005, the House of Representatives approved H. Res. 437, which created the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina (“the Select Committee”). According to the resolution, the Committee was charged with conducting “a full and complete investigation and study and to report its findings to the House not later than February 15, 2006, regarding (1) the development, coordination, and execution by local, State, and Federal authorities of emergency response plans and other activities in preparation for Hurricane Katrina; and (2) the local, State, and Federal government response to Hurricane Katrina.” The Committee presents the report narrative and the findings that stem from it to the U.S. House of Representatives and the American people for their consideration.

Report: <http://a257.g.akamaitech.net/7/257/2422/15feb20061230/www.gpoaccess.gov/katrinareport/mainreport.pdf>

Source: <http://katrina.house.gov/>

27. *February 15, Department of Homeland Security* — **Secretary Chertoff testifies on Hurricane Katrina response.** Department of Homeland Security Secretary Michael Chertoff testified on Wednesday, February 15, before the Senate Committee on Homeland Security and Governmental Affairs: "The scope of the damage is unprecedented — with some 90,000 square miles of impacted areas — an area larger than Great Britain and three-and-a-half times the area inundated by the Great Mississippi flood of 1927...The relief effort, of course, was also unprecedented. Within the first six days of the response, the Federal government delivered more than 28 million pounds of ice, eight and one-half million meals, and four million gallons of water. This exceeds the combined totals for the entire recovery operation during Hurricane Andrew."

Source: http://www.dhs.gov/dhspublic/interapp/testimony/testimony_0046.xml

28. *February 13, GovExec* — **Better training needed for emergency purchases, procurement, chief says.** Government officials need more training to respond effectively to sudden purchasing demands in emergency situations, an Office of Management and Budget official said Monday, February 13. Shortcomings in contingency contracting capabilities surfaced during last summer's hurricane season, said Robert Burton, acting administrator of OMB's Office of Federal Procurement Policy, at a conference hosted by the Arlington, VA-based Performance Institute. A lack of staff, particularly of managers and people experienced in handling emergencies, was a key problem at the Federal Emergency Management Agency and other agencies, he said. He noted that the Chief Acquisition Officers Council, a group of procurement chiefs, has established a working group on contingency contracting that is developing an outline of best practices for agencies to follow, as well as directories of individuals with expertise in emergency procurement and of existing contracts that could be relevant to future emergencies. While some lawmakers have called for more flexibility in federal acquisitions guidelines to respond to unanticipated events, knowledge of how to use the existing rules will be sufficient to meet agencies' contingency needs, Burton said.

Source: http://www.govexec.com/story_page.cfm?articleid=33383&dcn=to daysnews

[[Return to top](#)]

Emergency Services Sector

29. *February 14, KETV 7 (NE)* — **Nebraska introduces new response team.** Nebraska is better prepared in the event of a nuclear, chemical or biological attack now that the state has one of about a dozen homeland security teams certified by the Department of Defense. The mission of the 22 highly-trained National Guard soldiers out of Lincoln is to prepare and respond to the unthinkable. The team gets new high tech equipment to help its mission, including a mobile lab. A nuclear physicist will join the team, too. Together, they gather samples at the site of a suspected chemical or biological attack and determine at the scene whether weapons of mass destruction are present. The unit's commander unveiled the team on Tuesday, February 14. Lt. Col. Anita Curington will oversee \$3.3 million in equipment that officials said is crucial in protecting the safety of Nebraskans and first responders. Each member of the 22-person Nebraska Guard unit has averaged nearly 550 hours of training in preparation for the unit's approval. The unit is on-call 24 hours a day and has the ability to deploy to the scene of an incident within one hour.

Source: http://www.ketv.com/news/7055999/detail.html?rss=oma&psp=new_s

30. *February 14, Government Technology* — **Nebraska launches multi-county communications system.** On Friday, February 10, Nebraska Governor Dave Heineman launched the state's first regional, multi-county interoperable communications hub. The 10-county communications system allows the first responders and emergency service providers in central Nebraska to speak and share information across varied radio systems. The governor helped to develop Nebraska's state plan for bridging the gap between the different bands and brands of radio systems used by ambulance, fire, and police agencies. Nebraska's statewide communications plan calls for the continued development of similar regional radio network hubs that will eventually allow for an efficient statewide system of interoperable communications without the expense of replacing communications equipment. The new hub system uses radio and high-speed computer networks as a bridge.

Source: <http://www.govtech.net/news/news.php?id=98446>

31. *February 14, Portsmouth Herald (NH)* — **New Hampshire city receives auxiliary dispatch center grant.** A \$25,000 matching grant will provide Portsmouth, NH, with an alternative police dispatch center in case of an emergency. The grant, from the Federal Emergency Management Agency, required the city pay \$25,000 for the auxiliary center. The matching funds were paid with capital funds, allocated in 2003 to renovate the communications center. The money will be used to renovate storage space in the Public Works Complex into a fully equipped and furnished 24-foot by 24-foot dispatch center. "This redundant center would be set up so, if by natural disaster or physical attack we are unable to transmit information to fire and police, we can travel a short distance and within minutes be up and operating again," said Deputy Chief Len DiSesa.

Source: <http://www.seacoastonline.com/news/02142006/news/87696.htm>

[[Return to top](#)]

Information Technology and Telecommunications Sector

32. *February 15, VNUNet* — **Google 'hacking' occurs with the objective to find sensitive information on the Internet.** Malware authors are increasingly creating digital pests that use Google to find their next victim. Using the search tool for automated vulnerability detection is the latest trend in a technique known as 'Google hacking.' George Kurtz, senior vice president for risk management at security firm McAfee, told VNUNet about the phenomenon after a presentation at the RSA Conference in San José. The Santy.a worm, for instance, targeted a known vulnerability in some versions of the phpBB open source bulletin board application to deface Websites. It found its victims through an automated Google search query. Google eventually stopped the worm from spreading by blocking all searches that would turn up servers running the application. But the search engine is able to detect the abuse only if the queries stand out from other searches. Google 'hacking' does not mean breaking into the company's servers but involves online criminals using Google and other search engines to find sensitive information on the Internet.
Pictures and screenshots of 'Google hacks':
http://www.siliconvalleysleuth.com/2006/02/things_you_dont_h_tml
Source: <http://www.vnunet.com/articles/print/2150292>
33. *February 15, eWeek* — **Microsoft corrects security patch issue.** Microsoft was forced to update one of its February security patches after some users were unable to install the fix that addressed a TCP/IP vulnerability in several versions of Windows. The software giant confirmed on its Website that security patch number MS06-007 was altered to provide additional installation instructions after it was discovered that some people were having issues downloading the update. The company said the problem did not affect the content of the security patch itself. Microsoft said that shortly after the release of the patch on Tuesday, February 14, the company realized that the fix was not working properly when installed alongside its Inventory Tool for Microsoft Updates using its Automatic Updates, Windows Update, Windows Server Update Services and Systems Management Server 2003 management features.
Source: <http://www.eweek.com/article2/0,1895,1927250,00.asp>
34. *February 14, Arizona Daily Star* — **Romanian hacker breaks in to University of Arizona journalism computers.** Hackers broke into the computer system of the University of Arizona journalism department, and students were unable to use the computers Monday, February 13. All of the department's Apple Macintosh computers were affected and have been logged off the server and the Internet until the problem is solved, said Jacqueline Sharkey, head of the department. No information has been lost so far, she said. It was unclear Monday how long it would take to fix the security leak, she said. Department officials uncovered the problem during the weekend when they ran a security check on the computers. The computers are protected by a password, and Sharkey said she suspects that the hackers got through by trying "again and again and again." The security check showed that in other unrelated cases, hackers from Korea and Indonesia had tried to gain access to the system but were unsuccessful, she said.
Source: <http://www.azstarnet.com/metro/115789>
35. *February 14, Reuters* — **British computer hacker fights extradition to the U.S.** A British computer enthusiast accused by the U.S. government of the world's "biggest military hack of all time" began his court fight against extradition to the United States on Tuesday, February 14. Gary McKinnon was arrested in June last year on charges of computer fraud issued by U.S.

prosecutors claiming he illegally accessed 97 U.S. government computers — including Pentagon, U.S. Army, U.S. Navy and NASA systems. Prosecutors say he hacked into sensitive equipment over a one-year period from February 2002 and caused \$700,000 worth of damage, after crippling U.S. defense systems in the wake of the September 11 attacks. If found guilty, Mckinnon could face up to \$1.75 million in fines and 60 years in jail.

Source: http://today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2006-02-14T145400Z_01_L14737329_RTRUKOC_0_US-BRITAIN-USA-HACKER.xml&archived=False

- 36. February 14, Tech Web — Microsoft: IE zero-day bug not worth patching.** A new zero-day vulnerability in Internet Explorer (IE) is such a small deal, Microsoft said Tuesday, February 14, that it will not patch the bug, but instead will wait to fix it until it releases Windows XP SP3 in late 2007. The drag-and-drop flaw in IE 5.01, 5.5, and 6.0 was first reported to Microsoft in August 2005, and is somewhat similar to one addressed in a February 2005 security bulletin. "If an attacker can persuade a user to drag any object within the top-level window that his/her site is contained in, malicious script can redirect these inputs to other top-level windows, potentially resulting in an unintended consequence such as file installation," read an advisory published by SecuriTeam.

Microsoft IE Advisory issued by SecuriTeam:

<http://www.securiteam.com/windowsntfocus/5MP0B0UHPA.html>

Source: <http://www.crn.com/sections/breakingnews/dailyarchives.jhtml?articleId=180201596>

- 37. February 14, Tech Web — U.S. State Department launches Internet Freedom Task Force.** The U.S. State Department on Tuesday, February 14, established a task force to investigate the problems posed to the Internet by repressive regimes, a move that followed a call for help by Google Inc., Microsoft Corp. and Yahoo Inc., which have been criticized for censoring information in China. The task force would consider how the use of technology to restrict access to political content has impacted U.S. companies. The panel would also investigate the use of technology to track and repress dissidents and efforts to modify Internet governance structures in order to restrict the free flow of information. The task force is expected to draw upon the department's expertise in international communications policy, human rights, democracy, business advocacy, corporate responsibility and relevant countries and regions, Shiner said. Besides working with U.S. companies and non-governmental agencies, such as human rights groups, the task force will seek help from the European Union and other governments facing similar problems with Internet censorship.

Source: <http://www.techweb.com/wire/ebiz/180201737;jsessionid=U5ND2C KBMSPZ4QSNDBCCCKH0CJUMEKJVN>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT is aware of publicly available exploit code for a memory corruption vulnerability in the Mozilla Firefox web browser and Thunderbird mail client. If JavaScript is enabled in these applications, then the system is vulnerable to exploitation. A vulnerable system may be successfully exploited if a user is convinced to visit a specially crafted web page or open a specially crafted email.

A remote, unauthenticated attacker may be able to execute arbitrary code on a compromised system. If the user has elevated privileges, then the attacker will be able to exploit them. For more information please review the following US-CERT Vulnerability Note:

VU#759273 – Mozilla QueryInterface memory corruption vulnerability at URL: <http://www.kb.cert.org/vuls/id/759273>

US-CERT urges users and administrators to implement the following recommendations:

See update to Firefox 1.5.0.1 at URL: <http://www.mozilla.com/firefox/>

Please see SeaMonkey 1.0. at URL: <http://www.mozilla.org/projects/seamoney/>

Disable JavaScript in Thunderbird and Mozilla Suite.

Current Port Attacks

Top 10 Target Ports	1026 (win-rpc), 6881 (bittorrent), 25 (smtp), 445 (microsoft-ds), 18551 (---), 135 (epmap), 5274 (---), 139 (netbios-ssn), 32772 (sometimes-rpc7), 80 (www) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	--

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[\[Return to top\]](#)

General Sector

Nothing to report.

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.